公共安全平台详细设计

fort

2016年5月

1、引言

1.1、编写目的

公共安全平台详细设计是设计的第二个阶段，这个阶段的主要任务是在公共安全平台详细设计概要设计书基础上，对概要设计中产生的功能模块进行过程描述，设计功能模块的内部细节，包括算法和详细数据结构，为编写源代码提供必要的说明。

1.2、项目背景

由于现在项目很多，每个项目或多或少都需要权限控制。所以想到能不能把权限这一块公共出来，使其能够复用，由此诞生了这个公共安全平台。

1.3、参考资料

jhipster、Spring WebSocket Support

2、总体设计

2.1、需求描述

达到权限控制的基础功能，外部App使用FORT-SDK即可实现登录、注册、登出、用户信息修改、URL级别的权限控制、导航栏权限控制、不同一级域单点登录。同时，系统最大限度地实现易安装，易维护性，易操作性，运行稳定，安全可靠。

2.2、软件架构

系统由7大模块组成。分别是应用、资源、导航栏权限控制、权限、角色、用户、单点登录模块。

与SDK通信使用WebSocket，当已获得的数据有更新时，及时发消息到SDK。

2.3、规范

2.3.1、实体规范

如非特殊情况，每个实体都必须包含以下字段：

字段名	类型	验证	描述
id	Long	primary key	主键
createdBy	String	required maxlength(50)	创建人
createdDate	ZonedDateTime	required	创建时间

字段名	类型	验证	描述
lastModifiedBy	String	maxlength(50)	最后修改人
lastModifiedDate	ZonedDateTime		最后修改时间
st	String	maxlength(60)	冗余字段，备用

2.3.2、模块规范

如非特殊情况，开发者只能操作自己创建的数据

3、程序描述

3.1、应用(SecurityApp)模块

3.1.1、功能流程图

3.1.2、功能描述

开发者在本平台的管理后台CRUD应用

3.1.3、内部逻辑

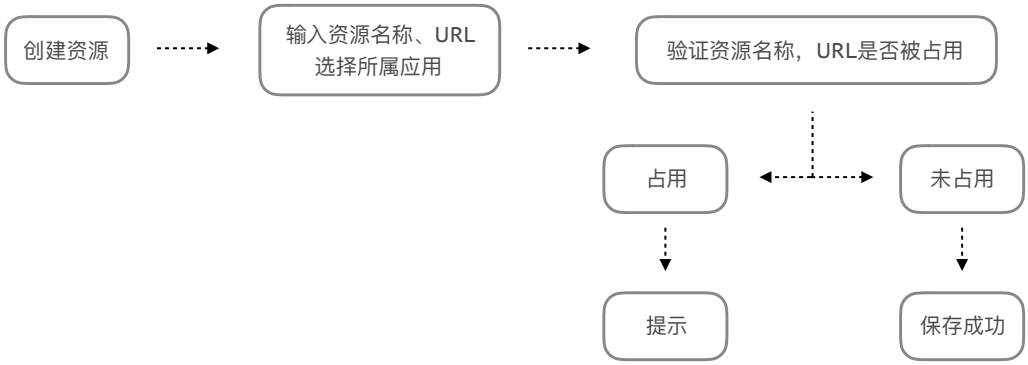
- 输入应用名称点击保存后即可获得随机生成的App Key、App Secret
- App Key、App Secret为自动生成的随机12位字母，且App Key、App Secret不可再修改
- 保存成功后创建一个用户名为App Key，密码为AppSecret的用户，角色为ROLE_SECURITY_APP

3.1.4、实体设计

字段名	类型	验证	描述
appName	String	required maxlength(50)	应用名称
appKey	String	maxlength(20)	App Key
appSecret	String	maxlength(20)	App Secret

3.2、资源(SecurityResourceEntity)模块

3.2.1、功能流程图



3.2.2、功能描述

开发者在本平台的管理后台管理应用的资源（URL）

3.2.3、内部逻辑

- 必须选择应用
- 资源名称，URL每个应用唯一
- 与应用是多对一关系

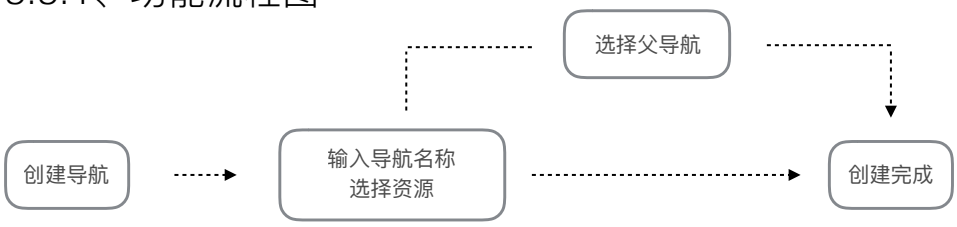
3.2.4、实体设计

字段名	类型	验证	描述
name	String	required maxlength(50)	资源名称
url	String	required	资源URL
description	String		描述

字段名	类型	验证	描述
app	SecurityApp	required	外键，应用

3.3、导航栏(SecurityNav)权限控制模块

3.3.1、功能流程图



3.3.2、功能描述

开发者在本平台的管理后台管理应用的导航栏
支持接收SecurityUser Token返回这个用户有权查看的导航栏

3.3.3、内部逻辑

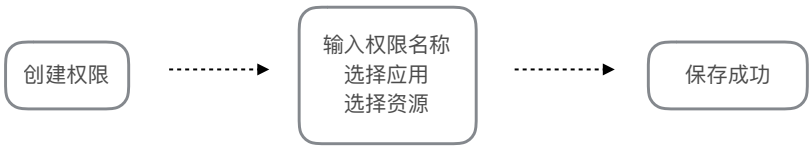
- 必须选择，且只能选择一个资源
- 导航栏有父子关系，可以无限继承，不允许循环继承
- 与资源是一对一关系
- 返回导航栏时，是树形结构

3.3.4、实体设计

字段名	类型	验证	描述
name	String	required maxlength(50)	导航栏名称
icon	String		图标
description	String		描述
parent	Long		父导航
resource	SecurityResourceEntity	required	外键，资源

3.4、权限(SecurityAuthority)模块

3.4.1、功能流程图



3.4.2、功能描述

开发者在本平台的管理后台管理应用的权限

3.4.3、内部逻辑

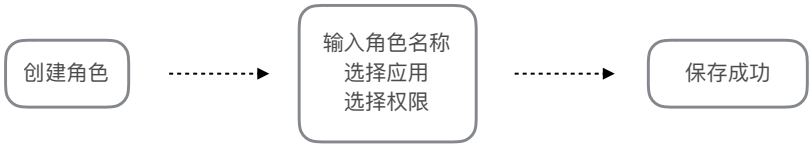
- 必须选择应用
- 选择应用之后才能选择资源，并且待选择的资源列表中只能包含已选择应用的资源
- 与应用是多对一关系，与资源是多对多关系

3.4.4、实体设计

字段名	类型	验证	描述
name	String	required maxlength(50)	权限名称
description	String		描述
app	SecurityApp	required	外键，应用
resources	Set<SecuritySource>	required	与资源的关系表

3.5、角色(SecurityRole)模块

3.4.1、功能流程图



3.4.2、功能描述

开发者在本平台的管理后台管理应用的角色

3.4.3、内部逻辑

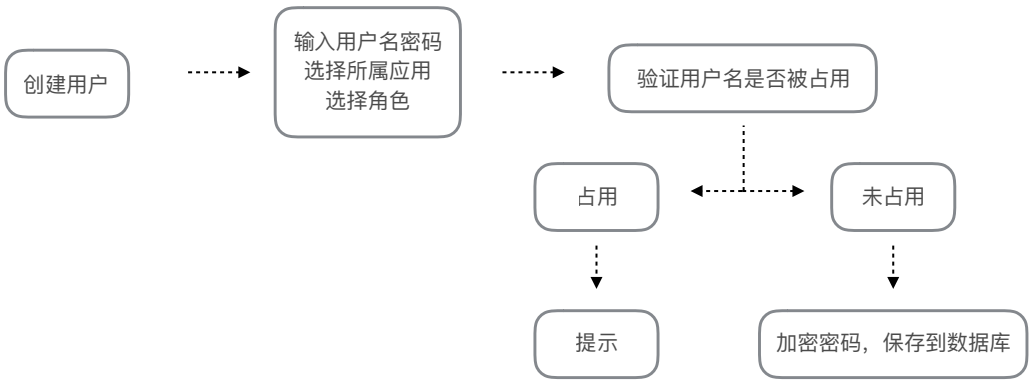
- 必须选择应用，选择应用之后才能选择权限，且待选择的权限列表中只能包含已选择应用的权限
- 与应用是多对一关系，与权限是多对多关系

3.4.4、实体设计

字段名	类型	验证	描述
name	String	required maxlength(50)	角色名称
description	String		描述
app	SecurityApp	required	外键，应用
authorities	Set<SecurityAuthority>	required	与权限的关系表

3.6、用户(SecurityUser)模块

3.2.1、功能流程图



3.2.2、功能描述

开发者在本平台的管理后台进行应用的用户管理。

3.2.3、内部逻辑

- 用户名在该应用内唯一
- 密码使用spring security BCryptPasswordEncoder加密
- 角色可以选择多个

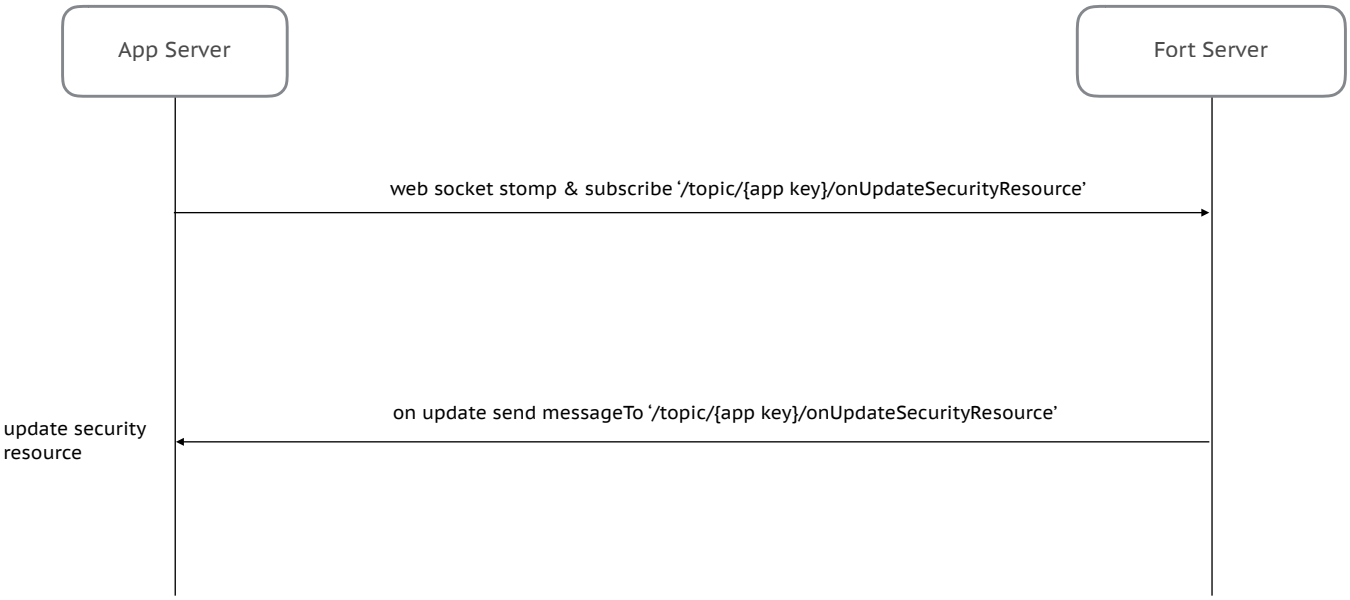
3.2.4、实体设计

字段名	类型	验证	描述
login	String	required maxlength(50)	登录名
passwordHash	String	maxlength(60)	密码的哈希值
email	String	maxlength(100)	邮箱
activated	Boolean	required	是否启用
app	SecurityApp		外键，应用
roles	Set<SecurityRole>		与角色的关系表

4、WebSocket

当资源更新时，发消息给App Server。当资源更新时，发送增量消息到这个资源的所属应用。

4.1、功能流程图



4.2、消息数据结构

消息通过String SONArray方式发送，每条消息的数据结构如下：

字段名	类型	描述
option	String	选项(RESTful风格)，新增：POST，更新：PUT，删除：DELETE
resourceClass	String	更新的资源类名

字段名	类型	描述
data	Object	数据